CalSAWS Job Description

Security Manager – Security Architecture & Data Protection

Salary Determined by Employer
RGS Salary Range:
$9,684.12 - $15,375.00 Monthly

JOB DESCRIPTION

We are seeking an experienced **Security Manager – Security Architecture & Data Protection** to strengthen our enterprise security program by ensuring security is built into technology, applications, data, and business processes from the start. Shift security left.

The successful candidate will lead security architectural reviews for new and changing technologies, evaluate security risks and design decisions, and establish effective controls to protect sensitive data.

The ideal candidate must be comfortable reviewing cloud architecture, challenging application design, evaluating an identity or integration pattern, discussing data flows with engineers, and explaining security risks and recommendations to leadership.

This role will report to the Chief Information Security Officer and partner closely with innovation, application, infrastructure, and other security and business teams.

RESPONSIBILITIES

Security Architecture & Design Review

Lead and perform security architectural reviews for new and existing systems, applications, infrastructure, integrations, cloud services, and technology initiatives.

Responsibilities include:

- Ensure security is incorporated into technology decisions early in the design lifecycle and ensure engineering teams implement secure-by-design practices.
- Maintain the security requirements for changes and ensure alignment with security best practices.
- Review solution architectures, application designs, data flows, integrations, APIs, network architectures, cloud environments. And technology implementations.
- Review of significant technology changes including cloud solutions, new platforms, SaaS solutions, APIs, integrations, CI/CD pipelines, and data sharing arrangements
- Identify security risks, design weaknesses, control gaps, and potential attack paths.
- Develop practical security architecture recommendations and compensating controls.
- Participate in architectural governance and security review boards as a security subject matter expert.
- Balance security requirements with operational, technical, business, and delivery considerations.
- Establish and continuously improve security architectural patterns, standards, reference architectures, and design principles.

Data Protection and Governance

Responsibilities include:

- Own and build a scalable data protection and governance program, strategy, and operating model ensuring data is accurate, consistent, and secure across enterprise.

- Execute a data protection strategy including DSPM coverage expansion, DLP maturity, and insider risk program.
- Own and oversee the discovery, classification, and risk assessment of CalSAWS data across all environments.
- Define and implement data governance policies aligned with privacy, security, compliance, and ethical AI standards.
- Provide strategy and direction for the full lifecycle of data protection controls spanning data in motion, data at rest, and data in use, across endpoint, cloud, email, and network channels.
- Support maturity of capabilities such as DLP, DSPM, encryption, tokenization, masking, access controls, and data discovery/classification.
- Review data retention, data minimization, access, sharing, and disposal practices from a security perspective.
- Oversee the development, deployment, and continuous tuning of DLP policies leveraging tools
- Develop and mature the behavioral analytics and detection capability for intentional and accidental data misuse, leveraging telemetry to identify anomalous data access, movement, and exfiltration patterns.
- Monitor emerging data security threats, technologies, and regulatory requirements and recommend improvements.
- Serve as subject matter expert on data security, data governance, data risk, AI/ML, and emerging data technologies.
- Provide governance oversight for major data programs, AI/ML initiatives, and digital transformation.
- Champion a data-driven and risk-based culture.
- Own the enterprise Insider Risk Program strategy, establish case management, investigation, and escalation protocols for insider risk incidents while preserving integrity and chain of custody.

QUALIFICATIONS AND REQUIREMENTS

MINIMUM QUALIFICATIONS

TRAINING AND EXPERIENCE:

- Graduation from an accredited college with a bachelor's degree in information security, Computer Science, Information Systems, Cybersecurity, or related field. Master's degree preferred.
- Six (6) years of progressively responsible, full-time, paid experience in security architecture, information security or data protection, with demonstrated depth in DSPM, DLP, and insider risk disciplines in a multi cloud environment, privacy, data security, or a similar operational role with at least two (2) years functioning in a supervisory capacity.
- Hands-on experience in performing security architecture and design reviews for complex enterprise systems, data protection -by-design, AI/ML systems, input/output monitoring, data residency enforcement, and access control.
- Strong understanding of authentication & authorization access controls, encryption, key management, secret management, network security, classification, retention, least privilege, logging & monitoring, vulnerability management, and secure software development.
- Working knowledge of privacy-by-design principles (data minimization, appropriate use, retention, transparency, and sharing constraints).
- Working knowledge of data security and security architectural reviews
- Experience working in large-scale enterprise or public-sector environments is strongly preferred.

- Experience supporting vendor onboarding, system/security reviews, procurement/TPRM processes, and data inventories/ROPA-style records.
- Experience managing structured workflows (intake, triage, documentation tracking, and closure) across multiple stakeholders.
- Strong organizational, documentation, and follow-through skills; able to manage multiple parallel requests and deliverables across stakeholders.
- Clear, concise written communication, including summaries, decision logs, and audit/client-ready documentation.
- Sound judgment with appropriate escalation of risks or uncertainties; high discretion in handling sensitive information.
- Ability to collaborate effectively with business, procurement, security, and compliance teams.

CERTIFICATIONS:

One or more of the following certifications is preferred:

- CISSP, CISM, CRISC, CCSP, CDPSE, CIPM or equivalent security certifications.
- GIAC certifications
- Security + or equivalent
- Cloud security certifications
- AWS Security Architect or equivalent

IDENTIFICATION:

A valid California Class C Driver License or the ability to utilize an alternative method of transportation when needed to carry out job-related essential functions.

PHYSICAL CLASS:

2 - Light.

OTHER REQUIREMENTS

N/A

SPECIALTY REQUIREMENTS

N/A